Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 2 | Issue : 3 | March 2016

NEW FINE-GRAINED UPDATES APPROACH FOR PUBLIC AUDITING DATA PRIVACY IN BIG DATA

Saudagar Shoaib [1] | Ranpise Ajit [1] | Nimbalkar Sushant [1] | Prof. Shrinivas Halhalli [1]

[1] Computer Science, G.S.M.C.O.E, Pune, India - 411045.

ABSTRACT

New concept in Information Technology is Cloud Computing, as it provides various scalable and elastic Information Technology services in pay-as-you-use basis, where the customers of cloud can reduce huge capital investments involved in IT infrastructure. Big data is an evolving term that describes any voluminous amount of structured, semi-structured andunstructured data, Cloud storage service is the cloud serviceswhich can provide a huge storage space to solve the bottleneck of the storage space of local end users, when the verification is done by a trusted third party, this verification process is also called data auditing and this third party is called an auditor, Compared to usersof conventional systems, cloud users need to surrender the local control of their datato cloud servers. Anotherchallenge for big data is the data dynamism which exists inmost big data applications. Due to the frequent updates, efficiency becomes a major issue in data management. As security always brings compromises in efficiency, it isdifficult but nonetheless important to investigate how to efficiently address securitychallenges over dynamic cloud data. Drawbacks First, a necessary authorization/authenticationprocess is missing between the auditor and cloud service provider, Second, although someof the recent work based on BLS signature can already support fully dynamic data updates over fixed-size data blocks, they onlysupport updates with fixed-sized blocks as basic unit, which we call coarse-grained updates.solutionsinevitably introduce a heavy computation overhead on the dataowner for key distribution and data management when fine grained data access control is desired.

KEYWORDS: cloud computing, big data, data security, provable data possession, authorized auditing, fine-grained data updates

Introduction

Cloud Computing in current Era is one of the influentialinnovations in computer science and technology in recent years. When the data size increasing, can mean that theprocessing time will be longer than the allotted time to process the data, In order to achieve an e clientverification ofdata integrity, the data owner can delegate a trusted thirdparty auditor (TPA) to assist the validation data reduction to consume the data owner's computing resources. In a remote verification scheme, the cloud storage server cannot provide a valid integrity proof of a given proportion of data to a verifier unless all this data is intact. To ensure integrity of user data stored on cloud service provider, this support is of no less importance than any data protection mechanism deployed by the cloud service provider (CSP), no matter how secure they seem to be, in that it will provide the verifier a piece of direct, trustworthy and real-timed intelligence of the integrity of the cloud user's data.

The service provider, whose target is to make a profit and maintain a reputation, has a reason to hide data loss. On the other hand, customers are very defective. Customers can openly or illegally claim loss to get paid. To avoid this independent, third party auditor will arbitrate and confirm whether stored and retrieved data is intact. we provide a formal analysis for possible types of fine-grained data updates and propose a scheme that can fully support authorized auditing and fine-grained update requests. Based on our schemewe also propose an enhancement that can dramatically reduce communication overheads for verifying small updates.

Problem Statement:

In the proposed research work we have to implement the system which provide the more data security with different file system. We work on text, Audio, Video and image also, and implement different kind of security algorithms.

Existing System

This system support fine-grained updates RSA signature is used, For integrity verification some algorithm is used like Merkle Hash Tree (MHT), advanced encryption standard (AES), Secure Hash Algorithm(SHA 1)

Disadvantages of existing system

Existing system have less security as compare to proposed system.Existing system provide security only for text data,Access permission only for single user.

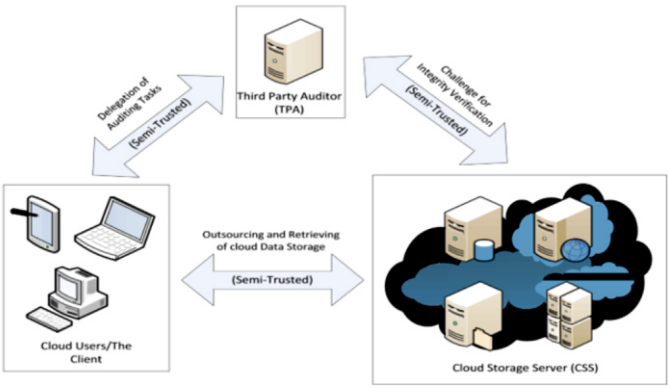
Proposed System

As data security is also considered as a metric of quality of service(QoS) along with other metrics such as storage and computation.Improve data security with different algorithm.Here we generate authentication key for multiple user. Also security for video, audio, image

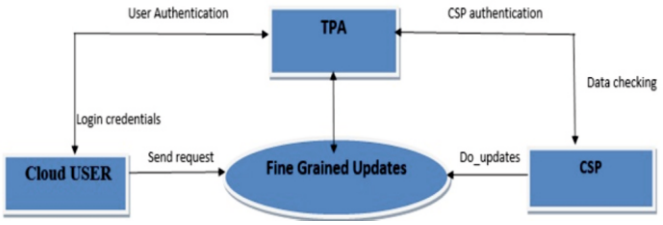
Advantages of proposed system

There are many advantages from proposed system like cost reduction, User friendly, More security Ease to use, Multiple user can access.

System Diagram:



Data Flow Diagram of Projects



Results

Many of project works developed previously which can only store data and share data between large numbers of users in a group. In our proposed work we have presented an third party auditing scheme to construct a secure data management mechanism with high privacy protection method and also working on auditability aware data scheduling scheme which is based on priority. We are developing our project in Netbeans IDE By using Java technology. We can analyze our system on the basis of security that we are providing. In the verification procedure of the scheme the emphasis is on preventing the CSS cheating the valid TPA about the status of user's data. Also the security of this scheme is enhanced by the use of a signature scheme that we are using in our system. Usually the schemes with signatures have a greater efficiency and are also more secure as compared to other systems. An invalid or unauthorized TPA is an outside auditor who wants to challenge the client's data stored onto the CSS without the permission of the client. This is not available in the earlier auditing schemes. Hence in this work with the unique authentication process no outside TPA without the user's permission can be able to audit the data without his

permission. Extending this security the user add a authentication message to make each auditing unique so as to avoid mix up results of auditing work between different auditors. Next the security analysis is to verify the updates over the client's data stored on the CSS. The analysis can be done here is whether the CSS (partially trusted) has carried out the data updates correctly or not. Here the updating the data the CSS must be able to honestly provide with the report on updates done on the data correctly. Also the CSS should be able to reduce the communication overhead for this process.

Conclusions:

Scalability/elasticity: As the cloud is a parallel distributed computing system in nature, scalability is one of the key factors as well Integrity verification.

Mechanism: that has the same level of scalability and elasticity will be highly resourceful for big data applications in a cloud environment.

Security: Security is always a problem between spear and shield; that is, attack and defend.

Efficiency: Due to high efficiency demands in big data processing overall, efficiency is one of the most important factors in designing of new techniques related to big data and cloud.

Acknowledgments:

We are profoundly grateful to Prof. Srinivas D, Project Co-Coordinators, for their expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. We are also grateful to Prof. Shrinivas Halhalli for his support and guidance that have helped us to expand our horizons of thought and expression. We would like to express our deepest appreciation towards Dr. F.B. Sayyed, Principal, G.S.MozeCollege of Engineering, Pune and Prof. J. Ratnaraj, Head of the Department, Computer Engineering Department whose invaluable guidance supported us in completing this project. At last we must express our sincere heartfelt gratitude to all staff members of Computer Engineering Department who helped us directly or indirectly during this course of work.

REFERENCES AND FOOTNOTES:

[1] Chang Liu, Jinjun Chen, Senior Member, IEEE, Laurence T. Yang, Member, IEEE Xuyun Zhang, Chi Yang, Rajiv Ranjan, and RamamohanaraoKotagiri, Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 9, SEPTEMBER 2014

[2] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud Computing and Emerging IT Platforms: Vision, Hype, Reality for Delivering Computing as the 5th Utility, Future Gen. Comput. Syst., vol. 25, no. 6, pp. 599-616, June 2009.

[3] M.Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, andM. Zaharia, AViewof Cloud Computing, Commun. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[4] Customer Presentations on Amazon Summit Australia, Sydney, 2012, accessed on: March 25, 2013. [Online]. Available: http:// aws.amazon.com/apac/awssummit-au/.

[5] J. Yao, S. Chen, S.Nepal,D. Levy, and J. Zic, TrustStore: Making Amazon S3 Trustworthy With Services Composition, in Proc. 10th IEEE/ACM Intl Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2010, pp. 600-605.

[6] D. Zissis and D. Lekkas, Addressing Cloud Computing Security Issues, Future Gen. Comput. Syst., vol. 28, no. 3, pp. 583-592, Mar. 2011.